cryptography

MDPI

Review

Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review

Hamed Taherdoost [1,2,*], Tuan-Vinh Le [3] and Khadija Slimani [4]

[1] Department of Arts, Communications, and Social Sciences, School of Arts, Science, and Technology, University Canada West, Vancouver, BC V6Z 0E5, Canada
[2] GUS Institute, Global University Systems, London EC1N 2LX, UK
[3] Bachelor's Program of Artificial Intelligence and Information Security, Fu Jen Catholic University, New Taipei 24206, Taiwan; tvle@mail.fju.edu.tw
[4] LDR Laboratory, Higher School of Computer Science Electronics and Automation (ESIEA), 75005 Paris, France; khadija.slimani@esiea.fr
* Correspondence: hamed.taherdoost@gmail.com

Abstract: With the rise in applications of artificial intelligence (AI) across various sectors, security concerns have become paramount. Traditional AI systems often lack robust security measures, making them vulnerable to adversarial attacks, data breaches, and privacy violations. Cryptography has emerged as a crucial component in enhancing AI security by ensuring data confidentiality, authentication, and integrity. This paper presents a comprehensive bibliometric review to understand the intersection between cryptography, AI, and security. A total of 495 journal articles and reviews were identified using Scopus as the primary database. The results indicate a sharp increase in research interest between 2020 and January 2025, with a significant rise in publications in 2023 and 2024. The key application areas include computer science, engineering, and materials science. Key cryptographic techniques such as homomorphic encryption, secure multiparty computation, and quantum cryptography have gained prominence in AI security. Blockchain has also emerged as an essential technology for securing AI-driven applications, particularly in data integrity and secure transactions. This paper highlights the crucial role of cryptography in safeguarding AI systems and provides future research directions to strengthen AI security through advanced cryptographic solutions.

Keywords: artificial intelligence; authentication; blockchain; cybersecurity; data privacy; machine learning; quantum cryptography

Academic Editor: Josef Pieprzyk

Received: 26 January 2025
Revised: 25 February 2025
Accepted: 4 March 2025
Published: 7 March 2025

Citation: Taherdoost, H.; Le, T.-V.; Slimani, K. Cryptographic Techniques in Artificial Intelligence Security: A Bibliometric Review. *Cryptography* **2025**, *9*, 17. https://doi.org/10.3390/cryptography9010017

1. Introduction

Despite the significant advancements in artificial intelligence (AI) over the past few years, there is a dearth of discourse regarding the security of systems [1]. Consequently, it is advantageous to be informed of the most recent developments in the subject matter in order to chart the field's progress and the subsequent results [2]. The security of AI is an important priority because it contributes to minimizing risks and safeguarding very critical systems and data, which are susceptible to continuous interference by AI in technology development [3].

AI security is the set of policies and procedures put in place to protect the AI systems from adversarial attacks that may alter the AI system to produce incorrect results or result in manipulation of data integrity. According to Parmar [4], strong security is paramount, especially for mission-critical systems relying on AI-driven decision-making processes,

in the Explainable AI Security discussion. AI security needs to be built on explainability-transparency, trust, and the ability for stakeholders to understand why an AI-driven choice has been made.

A crucial constituent in securing the AI systems with cryptography, it contains the tools and instruments that preserve private information on legitimacy, confidentiality, and integrity. Many AI systems tend to process data in volumes. Thus, it calls for methods in cryptography that assure the integrity and non-disclosure of the data processed. For example, lightweight cryptography has gained importance for resource-constrained situations regarding IoT and ensuring security for various AI applications [5].

Strong cryptographic techniques are becoming more and more necessary to safeguard sensitive data and algorithms as the usage of AI spreads throughout a number of industries, including cybersecurity, healthcare, and finance. To protect financial data and transactions, the study underlined the necessity of thorough security measures, including cryptographic techniques. A bibliometric re-examination of the Internet of Things (IoT) on cybersecurity issues was carried out by Ganji and Afshan [6], which provided insight into research trends and gaps in this crucial field. The study emphasized how crucial it is to adopt encryption techniques and other security measures to address security issues in IoT devices. The use of blockchain technology and artificial intelligence in business creates both new security opportunities and challenges [7]. The integration of AI with business highlights the significance of addressing gaps in the current literature in order to improve the security of AI systems in a range of business applications [8]. All things considered, the value of cryptographic methods in guaranteeing the safety of AI systems in various industries is becoming increasingly acknowledged. To improve the security of AI systems and shield private information and algorithms from online attacks, it is imperative to fill in the gaps in the current literature by thorough investigation and analysis.

New fields of study often identify key deficiencies that require further investigation. In the case of the study on decision support systems in search and rescue operations by Nasar et al. [9], one finding was a deficiency in research studies relating to maritime applications; this suggests further studies are needed in this key domain. The fact that there are no quantitative and qualitative bibliometric analyses with regard to oxidative stress and pulmonary disorders, as pointed out by Liu et al. [10], indicated a huge area for further investigation.

Despite the advancements in AI security, the literature lacks a consolidated analysis of cryptographic techniques applied in AI security frameworks. This paper addresses this gap by conducting a bibliometric review to identify key research trends, techniques, and challenges in cryptographic applications for AI security. The study aims to provide insights into the development of secure AI systems, focusing on critical cryptographic techniques, their implementation, and their impact on enhancing AI security. The bibliometric review methodology enables a structured analysis of the literature, identifying influential research works, emerging trends, and research gaps. This study contributes to the field by offering a comprehensive understanding of the role of cryptographic techniques in AI security and outlining future directions for research and development.

The paper primarily aims to conduct a bibliometric review for the investigation of the relationship between cryptographic methods and AI security by offering an in-depth analysis of major themes, trends, and seminal works in this fast-developing subject. This paper seeks to identify the trends and highlight new research areas, considering the most used cryptographic techniques in AI security, their geographical diffusion, and historical evolution. The current paper, therefore, seeks to critically evaluate the contribution of top authors and organizations, identify the networks of citation, and also assess the general

impact that cryptography makes on AI security for an insightful overview of the current issues at present and a probable direction for future research in the field.

2. Materials and Methods

Since it is a versatile tool, the bibliometric techniques can be set in place within a wide array of disciplines, including the social sciences, management, and healthcare. A bibliometric analysis, which has assessed the efficacy of different counting techniques along with the frameworks in management research, shed light on the methodological rigor of past research [11]. Similarly, bibliometric methods have been applied in the healthcare industry to evaluate patient satisfaction with treatments, which shows disparities, hence further areas of development [8].

Another strong rationale for adopting a bibliometric method is data visualization. Using keyword clustering and co-citation analysis, for instance, researchers can visually depict the relations of various studies. This was well pointed out in a bibliometric study that, through visualized keyword networks, portrayed the evolution of the literature on lean management over time so as to identify trends and clusters [12].

In short, the bibliometric technique is chosen because it can provide a structured and quantitative assessment of scientific publications. This approach has a number of benefits: it identifies influential works, visualizes research trends, identifies areas of research gaps, and many more. Quite a large number of studies, ranging from psychological skills training to sustainable urban development, prove that bibliometric analysis provides a clear device for researchers who want to make sense of and negotiate the complexities of their respective fields [13,14].

Using the following keywords, the Scopus database was searched for pertinent literature: TITLE-ABS-KEY (“artificial intelligence” OR AI), TITLE-ABS-KEY (cryptography), AND TITLE-ABS-KEY (security). There were 3010 documents found. The corpus was reduced to 495 pertinent documents by concentrating exclusively on journal articles and reviews written in English and published between 2020 and the present (January 2025). Since these materials were taken from well-known scholarly resources, studies that were published in peer-reviewed journals were thoroughly covered. This study visualized the gathered literature keywords data using VOSviewer 1.6.20 Version. To give an up-to-date analysis of the trends in the field, the data collection was restricted to articles published up until the present year.

3. Results

The record clearly shows that research on cryptographic strategies in AI security is growing at a fast pace in the last few years, thereby reflecting the increasing importance of this multidisciplinary topic (Figure 1). It similarly showed a fivefold increase in four years—from 32 in 2020 to 161 in 2024—indicating a consistent growing trend in publication output. It develops the trend to show interest in the upscale of developing a secure and private AI system while the applications of AI into critical sectors such as healthcare, financial institutions, and defense are increasing. More important is the increase in the number of publications in 2023 with 134 papers and 2024 with 161 documents, probably due to increased cryptography techniques and the capability of AI; now, on this topic, there is more awareness globally as a result of the growing need to address security flaws associated with AI.

Because there have already been five publications, this reflects continuity and constant interest in the issue of publication by researchers in the year January 2025 alone. Given that now everything around is undergoing huge digital changes, such a tendency enhances the need to enable powerful cryptography inclusion in AI systems to care for security

and data protection. The combination of factors, including development in AI technology, increased regulatory attention to the protection of data, and the need to reduce the dangers of adversarial attacks on AI models, probably explains the steep rise in publications beyond 2020.

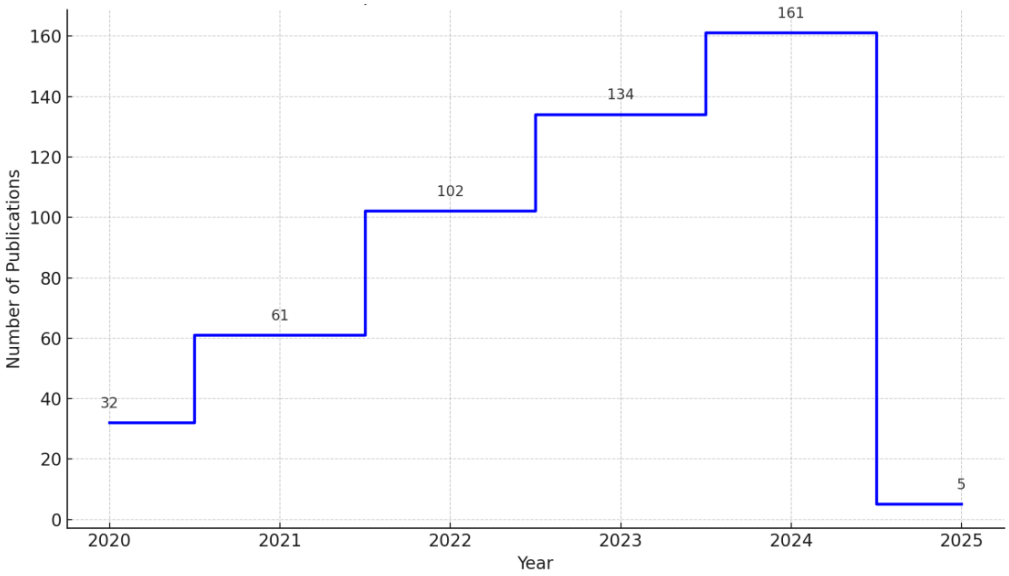

Figure 1. Number of documents included over last five years.

From the document types analysis, 452 of the 603 documents analyzed are research articles and, therefore, the most representative in the publications of the topic cryptographic techniques in AI security. The prevalence of original research would denote high attention toward state-of-the-art developments and innovative contributions proposed so far to merge AI with cryptography to solve security issues. Reviews, on the other hand, are just 43 documents—a relatively small yet equally important collection of works whose purpose is to identify gaps in research and synthesize knowledge. The large volume of research articles indicate that research is highly active and vibrant, with the main efforts directed at the investigation of advanced cryptography techniques, creation of safe AI systems, and solving real-world implementation issues.

While revealing the technical and fundamental character of the subject area (Figure 2), most of the analyzed documents on cryptographic techniques in AI security fall under computer science, numbering 400 documents, and engineering with 271 documents. In this regard, it denotes the contribution which the discipline holds in terms of contributing toward secure AI frameworks, privacy-preserving technologies, and cryptographic techniques. In a related way, the big contribution of engineering underlines the applied character of embedding these techniques in real systems and applications. Leaving aside these foundational disciplines, materials science is strongly represented, with 88 documents, followed by mathematics, with 80 documents, probably due to their applicability in developing mathematical models required for safe AI systems and hardware-based cryptography solutions. Including physics and astronomy may suggest that advanced computational methods from physical systems are borrowed in order to contribute to developing cryptographic protocols in AI with 65 papers.

Other subject areas, such as chemistry with 33 documents, and biochemistry, genetics, and molecular biology with 31 documents, reflect the interdisciplinary use of cryptography in the area of secure AI applications in bioinformatics and chemical data processing. This is further supported by the contribution from business, management, and accounting with 18 documents, while 19 documents were found within the social sciences. It shows a

growing interest in managerial and sociotechnical aspects for the integration of secure AI systems within organizational contexts. While the contribution of disciplines like medicine with 7 documents and neuroscience with 3 documents shows that an effort has been made to protect data privacy and security in healthcare AI applications, the presence of decision sciences with 17 documents is indicative of the growing demand for secure decision-making frameworks in AI.

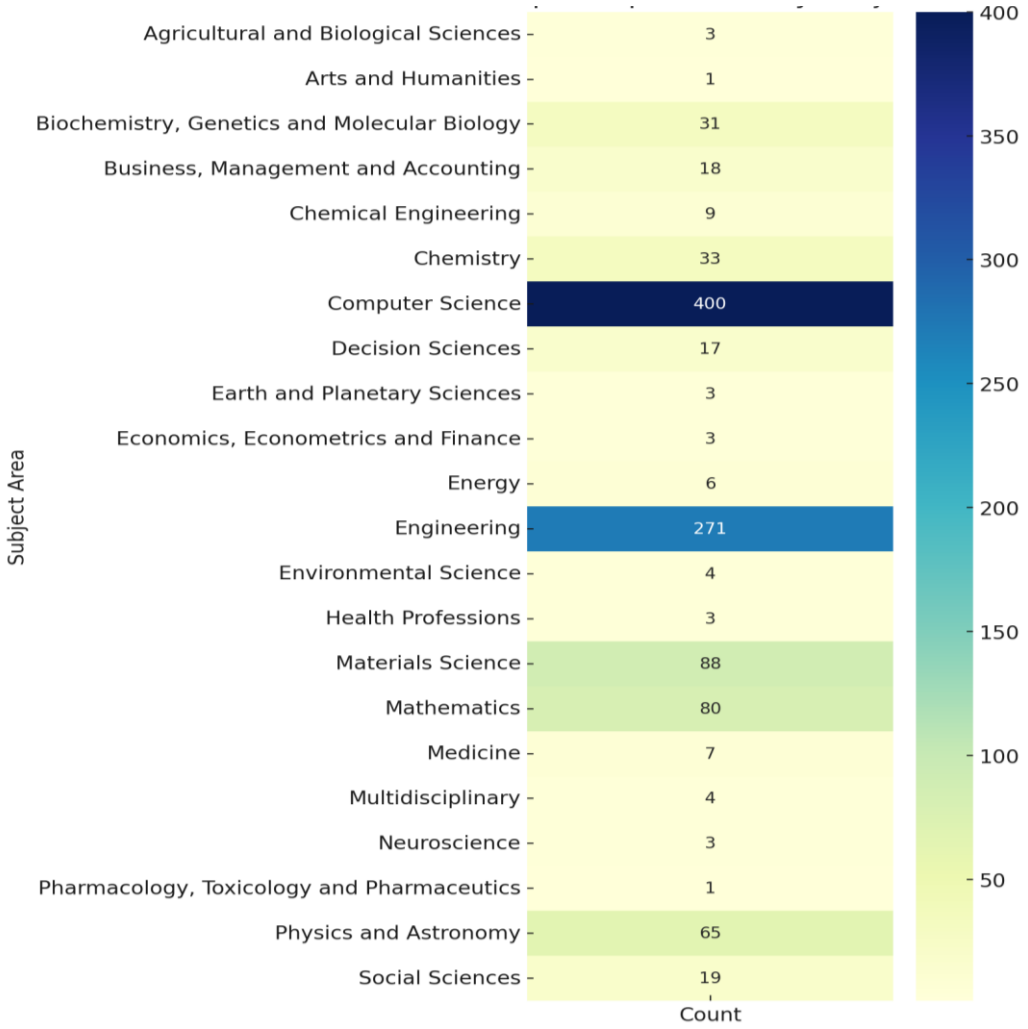

Figure 2. Fields' distribution of documents included.

The authors' geographic distribution shows that cryptographic techniques in AI security are highly popular worldwide, with Asia making major contributions (Figure 3). Strong research activity is seen in China and India, as China leads with 161 publications while India comes in second with 143. Their quick developments in AI and cryptography, along with large expenditures in technology and cybersecurity infrastructure, are the reasons for their dominance. With 76 articles, Saudi Arabia comes in third place, demonstrating its growing emphasis on technical innovation and safe AI frameworks as a component of its national development plans. The contributions made by the United States (51) and the United Kingdom (36) highlight the significance of these nations as research centers, with a particular focus on developing cryptographic techniques to tackle the security issues of AI systems.

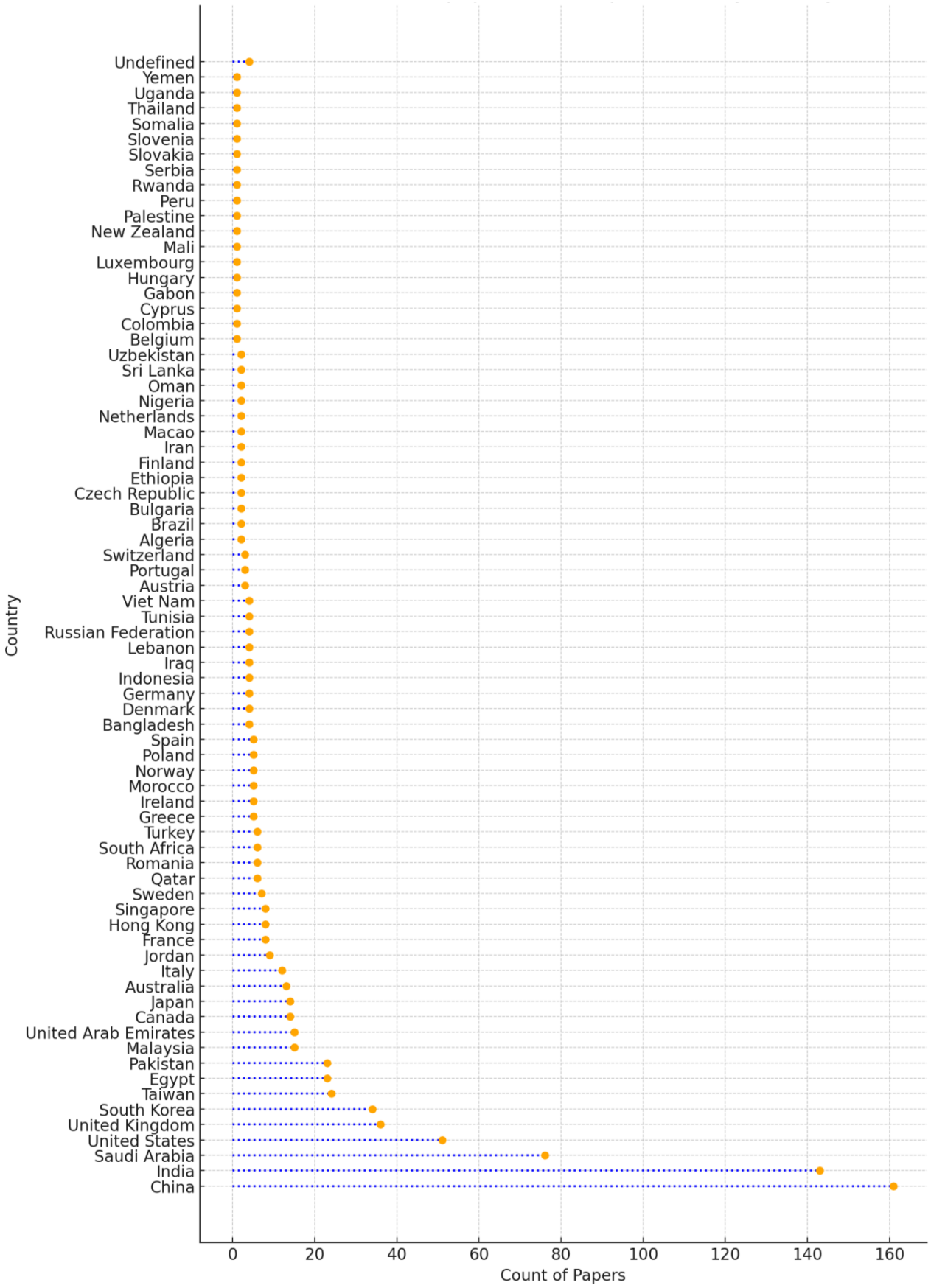

Figure 3. Countries of documents' authors.

Notable activity is demonstrated by nations like South Korea (34), Taiwan (24), and Egypt (23), as a result of academic and commercial efforts in AI security. Growing regional research efforts in the Middle East and South Asia are highlighted by the 15 or more articles contributed by Pakistan, Malaysia, and the United Arab Emirates. The contributions from Japan (14) and Canada (14) further illustrate how knowledge in this area is distributed throughout the world. Although they are represented, European countries, including Italy (12), France (8), and Germany (4), have very low publication numbers, suggesting room for more engagement in this field. The existence of nations like South Africa, Qatar, and Turkey highlights the growing interest in safe AI systems in a variety of geographical areas.

The institutional affiliations analysis reveals a wide variety of contributors to the field of cryptographic techniques in AI security as shown in Table 1, with a significant presence from universities and research institutes in Saudi Arabia, China, and India. The list is topped by King Abdulaziz University, which has 13 publications. King Saud University and Taif University are in close proximity, each contributing 12 publications. The country's emphasis on the advancement of AI and cybersecurity research is emphasized by the dominance of Saudi institutions, which is consistent with its overarching vision of technological innovation and leadership in the Middle East. These universities are likely to be able to investigate cutting-edge cryptographic techniques to improve AI security due to the substantial government funding and collaborative opportunities they receive.

Table 1. Top 12 Affiliations' Distribution.

Affiliation	Number of Publications
King Abdulaziz University	13
King Saud University	12
Taif University	12
Chinese Academy of Sciences	10
SRM Institute of Science and Technology	9
Prince Sattam Bin Abdulaziz University	9
Peng Cheng Laboratory	9
Beijing University of Posts and Telecommunications	8
University of Petroleum and Energy Studies	8
Ministry of Education of the People's Republic of China	7
Vellore Institute of Technology	7
Nirma University	7

Institutions in China also make substantial contributions, with the Chinese Academy of Sciences producing 10 publications and entities such as Peng Cheng Laboratory and Beijing University of Posts and Telecommunications contributing 9 and 8 publications, respectively. These figures are indicative of China's substantial investment in AI (AI) and cryptography, which is motivated by national strategies to safeguard technological advancements. In the interim, Indian institutions such as Vellore Institute of Technology (7), University of Petroleum and Energy Studies (8), and SRM Institute of Science and Technology (9), are demonstrating an increasing emphasis on AI security research. The interdisciplinary and collaborative nature of research in this discipline is underscored by the presence of Prince Sattam Bin Abdulaziz University (9) and other institutions.

It also was observed from the author analysis that various researchers have contributed notably to research in cryptographic techniques in AI security (Table 2). The highest number of authored books by a single contributor, A.K. Das has contributed to seven books, and his high publication count depicts significant influence and continuity in the advancement of the research on the integration of cryptography and AI security. The

ongoing research efforts of important persons are further highlighted by authors like S. Tanwar (7 publications), P. Vijayakumar (6 publications), and N.K. Jadav (5 publications), who have all contributed to the creation of secure AI frameworks through advancements in cryptography. These writers are most likely spearheading or taking part in cooperative research projects that advance the theoretical and applied facets of employing cryptography approaches to secure AI systems.

Table 2. Top 12 authors.

Author	Number of Publications
Das, A.K.	7
Tanwar, S.	7
Vijayakumar, P.	6
Jadav, N.K.	5
Alshehri, M.D.	4
Dev, K.	4
Gupta, D.	4
Gupta, R.	4
Kumar, N.	4
Shankar, K.	4
Veeravalli, B.	4
Wazid, M.	4

M.D. Alshehri, K. Dev, D. Gupta, R. Gupta, N. Kumar, K. Shankar, B. Veeravalli, and M. Wazid are other noteworthy contributors with several publications, each with four. These scholars show both individual and group contributions to the area, representing a broad group from different institutions. Their works likely touch on everything—from the development of algorithms to research that puts emphasis on certain applications in AI-driven systems. By the density of the authors' publications, a conclusion may be made that they are players in the current study on the use of cryptography in securing AI and that through their works they put forward thought-provoking opinions and practical solutions to further scientific understanding in this multidisciplinary area.

As illustrated in Table 3, with 47 articles published, IEEE Access is the top publication outlet for research on cryptographic algorithms in AI security, according to the journal study. This indicates IEEE Access's important role as a major platform for multidisciplinary technology and cybersecurity research. The IEEE Internet of Things Journal (14 publications) and Sensors (21 publications) are two more noteworthy journals that show a keen interest in using cryptographic techniques to secure sensor networks and the Internet of Things (IoT), which are crucial parts of contemporary AI systems. Specialized research on protecting multimedia systems and wireless communications in the context of AI is published in journals including Security and Communication Networks (8), Multimedia Tools and Applications (8), and Wireless Personal Communications (10). The emphasis on protecting sensitive data and hardware-based solutions in AI applications is highlighted by the existence of journals such as IEEE Transactions on Information Forensics and Security and Computers Materials and Continua (both with seven publications).

Key term analysis shows major areas of interest in the interface between security, artificial intelligence, and cryptography (Figure 4). A very close linkage between AI and network security shows the importance of secure AI-based systems and stringent mechanisms of the security mechanism within communication networks. Because cryptography is the main supporter in protecting AI applications, it remains a pressing issue. Other key topics include the Internet of Things, where the protection of the linked devices is now a big concern; machine learning; blockchain; authentication, where cryptographic protocols are investigated to improve data integrity, system privacy, and secure communication.

Table 3. Top 10 journals.

Journal	Number of Publications
IEEE Access	47
Sensors	21
IEEE Internet Of Things Journal	14
Wireless Personal Communications	10
Multimedia Tools and Applications	8
Security And Communication Networks	8
Computers Materials and Continua	7
IEEE Transactions on Information Forensics and Security	7
Wireless Communications and Mobile Computing	7
International Journal of Advanced Computer Science and Applications	6

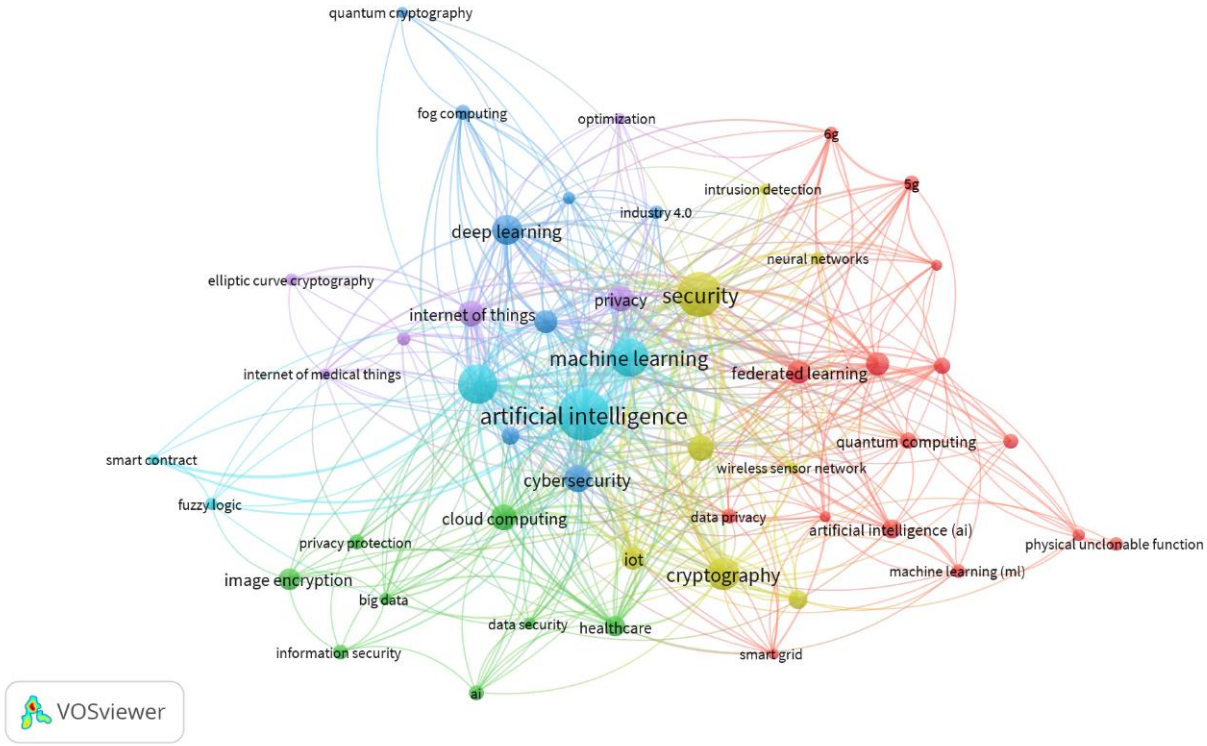

Figure 4. Cluster of keywords (Created using vosviewer.com accessed 5 January 2025).

Developing areas like post-quantum and quantum cryptography feature at the same time, demonstrating that the protection of AI systems against potential quantum computing dangers is becoming increasingly important. Other major concerns involve cybersecurity and data privacy, showing the need to protect private data in AI settings. The growth of cloud and edge computing illustrates the shift toward decentralized AI models, which have high-priority needs for security preservation across distributed systems. The use of cryptographic techniques to contribute to the security and privacy of machine learning models underlines such topics as federated learning, neural networks, and intelligent systems, further advancing the development of secure AI systems.

The authors' publications highlight significant contributions to the intersection of AI, cryptography, and security, particularly in emerging fields like IoT, 5G, and healthcare (Table 4).

Table 4. Top cited papers in each single year (2020 to 2024).

Authors	Title	Year	Source Title	Cited by
Fang et al. [15]	Orbital angular momentum holography for high-security encryption	2020	Nature Photonics	586
Taylor et al. [16]	A systematic literature review of blockchain cyber security	2020	Digital Communications and Networks	417
Tange et al. [17]	A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities	2020	IEEE Communications Surveys and Tutorials	302
Khan et al. [18]	6G Wireless Systems: A Vision, Architectural Elements, and Future Directions	2020	IEEE Access	259
Sharma et al. [19]	Communication and networking technologies for UAVs: A survey	2020	Journal of Network and Computer Applications	229
Anuradha et al. [20]	IoT enabled cancer prediction system to enhance the authentication and security using cloud computing	2021	Microprocessors and Microsystems	112
Zaman et al. [21]	Security Threats and Artificial Intelligence-Based Countermeasures for Internet of Things Networks: A Comprehensive Survey	2021	IEEE Access	94
Li et al. [22]	Research on AI security enhanced encryption algorithm of autonomous IoT systems	2021	Information Sciences	83
Sharma et al. [23]	Role of machine learning and deep learning in securing 5G-driven industrial IoT applications	2021	Ad Hoc Networks	83
Jan et al. [24]	Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS	2021	IEEE Transactions on Industrial Informatics	81
Razdan and Sharma [25]	Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies	2022	IETE Technical Review (Institution of Electronics and Telecommunication Engineers, India)	188
Hasan et al. [26]	A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things	2022	IET Communications	140
Almaiah et al. [27]	An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems	2022	Sensors	109
Abdel Hakeem et al. [28]	Security Requirements and Challenges of 6G Technologies and Applications	2022	Sensors	102
Neelakandan et al. [29]	Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model	2022	International Journal of Modeling, Simulation, and Scientific Computing	75
Rajapaksha et al. [30]	AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey	2023	ACM Computing Surveys	79
Boualouache and Engel [31]	A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks	2023	IEEE Communications Surveys and Tutorials	55
Friha et al. [32]	2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT	2023	Computers and Security	53
Deebak et al. [33]	A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems	2023	IEEE Internet of Things Journal	52
Ein Shoka et al. [34]	An efficient CNN-based epileptic seizures detection framework using encrypted EEG signals for secure telemedicine applications	2023	Alexandria Engineering Journal	48
Almalawi et al. [35]	Managing Security of Healthcare Data for a Modern Healthcare System	2023	Sensors	48
Dhar Dwivedi et al. [36]	Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions	2024	Transactions on Emerging Telecommunications Technologies	61
Gill [37]	Quantum and blockchain-based Serverless edge computing: A vision, model, new trends and future directions	2024	Internet Technology Letters	41
Alqaralleh et al. [38]	Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment	2024	Personal and Ubiquitous Computing	30
Pleshakova et al. [39]	Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends	2024	Journal of Computer Virology and Hacking Techniques	19
Fang et al. [40]	Toward Secure and Lightweight Data Transmission for Cloud-Edge-Terminal Collaboration in Artificial Intelligence of Things	2024	IEEE Internet of Things Journal	19

4. Discussion

The objective of the convergence of AI and cryptography is to develop security measures that are more adaptable and intelligent [41]. This integration also introduces new

challenges, such as vulnerabilities in traditional cryptographic algorithms that can be exploited by quantum computers. Quantum computing poses a threat to conventional cryptographic methods, including symmetric key encryption (e.g., AES) and asymmetric key encryption (e.g., RSA), which are extensively employed. Quantum-resistant or post-quantum cryptography is currently being developed to mitigate these vulnerabilities. Quantum cryptography, which is founded on the principles of quantum mechanics, provides unconditional security; however, it necessitates substantial infrastructural investments. The integration of quantum cryptography with neural networks improves the efficacy of the development of robust cryptographic protocols [42]. By identifying patterns in ciphertexts, machine learning models can perform automated cryptanalysis, potentially exposing vulnerabilities in existing algorithms [41,43]. This capability underscores the potential advantages of employing AI-driven methodologies to fortify cryptographic systems and the dangers posed by adversarial attacks on traditional cryptography. In collaborative environments, where multiple parties require access without jeopardizing data secrecy, advanced secure collaboration protocols are essential. These protocols utilize machine learning techniques to identify anomalies while simultaneously safeguarding confidentiality [41]. Table 5 illustrates the relevance of AI security cryptography methods in data integrity, confidentiality, and secure communication by comparing them across various application areas.

Table 5. Comparison of cryptographic techniques for AI security.

Study	Cryptographic Technique Used	Application Context	Key Findings
Pramanik et al. [44]	Steganography + Cryptography	Business intelligence security	Faster and more accurate than existing methods
Dai and Boroomand [45]	AI-Enhanced Security Models	Big Data security	Evaluated security threats and defense strategies
Al-Suqri and Gillani [46]	Cryptographic Security Models	National security	Emphasized AI's role in mitigating cyber threats
Gulo et al. [47]	Cryptographic AI Protection	Economic and security contexts	Highlighted AI security risks in geopolitical trade wars
Pise et al. [48]	AIoT Cryptographic Protocols	Healthcare security	Addressed privacy and integrity concerns in AIoT healthcare
Hegde et al. [49]	Quantum Cryptography	Secure communication	Compared classic vs. quantum cryptographic techniques

While cryptography methods play an essential role in securing AI systems, various challenges associated with their broad applications reduce the rate of usage. One main challenge that sophisticated cryptographic methods involve: the high computation costs. According to Fang et al. [15], computational resource-intensive techniques—like homomorphic encryption—allow conducting computations on encrypted data; due to its higher CPU demand, its practical applicability to real-time AI is also quite unrealistic. While large-scale systems are those for which cloud-based AI frameworks need to have millions of concurrent transactions securely dealt with, the scalability of cryptography enablers is another challenge. Most of the existing techniques provide an inadequate balance between security and performance. Bottlenecks hinder the performance in most situations and reduce overall effectiveness [18].

There are still implementation issues, particularly in integrating cryptography techniques in various AI systems. For example, many times it requires a lot of customization to ensure full compatibility between AI algorithms and the standards for security, which increases costs and development time [17]. The existing cryptography techniques are being strained by the emerging risks, such as quantum computing. Although essential, some

of the basic algorithms, such as RSA and ECC, will no longer be valid in the event of quantum-based attacks; hence, post-quantum cryptography techniques should be taken up immediately [50]. Now is the time to invent new strategies for cryptography design, keeping efficiency, scalability, and adaptability on the frontline.

Notwithstanding these obstacles, there is a great deal of promise for future developments in cryptographic methods specifically suited for AI security. For resource-constrained contexts like edge computing and the Internet of Things, where conventional methods are impracticable, research into lightweight cryptographic techniques has promise [25]. These methods seek to maximize security without sacrificing AI systems' functionality. The creation of hybrid cryptographic models, which blend conventional and quantum-resistant algorithms to offer multilayer security and guarantee resilience against new attacks, is another field that is ready for innovation [26].

The development of cryptography may change with the development of AI and machine learning. AI-driven models optimize anomaly detection and generation of cryptographic keys, hence allowing more effective and flexible security protocols [51]. Federated learning ensures data privacy across dispersed systems while easily integrating advanced cryptographic techniques into AI frameworks. Zero-knowledge proof could find broader applications in AI security; this allows verification of a calculation without necessarily releasing private information. Yu et al. [52] discuss this issue. Thus, the interaction between AI and cryptography provides, in itself, a method to bring into consideration next-generation security solutions that will be effective against new kinds of threats.

The integration of AI-driven anomaly detection with cryptographic security, emergent threats such as Large Language Model (LLM)-based vulnerabilities, and the limited focus on real-time cryptographic AI security solutions are among the numerous research gaps that remain unaddressed. Real-time cryptographic AI security solutions have been acknowledged for their capacity to dynamically modify encryption protocols in response to dynamic threat landscapes and data sensitivity. These systems employ machine learning algorithms to analyze transaction patterns in real time, thereby identifying potential hazards and optimizing encryption processes accordingly [53]. In spite of these developments, there is a requirement for more thorough research to investigate the most effective methods for optimizing these systems for a variety of environments and scaling them without sacrificing performance.

The application of Large Language Models (LLMs) to cybersecurity tasks, including malware analysis and vulnerability detection, is on the rise [54]. Nevertheless, LLMs also introduce new vulnerabilities that necessitate further investigation. A more profound comprehension of the ways in which cryptography can mitigate these risks is required due to the use of LLMs in the generation of sophisticated attacks or the exploitation of vulnerabilities in existing systems [55]. The development of cryptographic methods that are specifically designed to counteract LLM-based threats is a research lacuna.

Powerful tools for identifying uncommon patterns that may indicate cyber threats are provided by AI-driven anomaly detection. This capability could be integrated with cryptographic security to improve the efficacy of encryption systems by autonomously adjusting their strength in response to anomalies that are detected. Although some studies have conceptualized this integration, there is a scarcity of practical implementation research. To develop robust frameworks that seamlessly integrate adaptive encryption techniques with anomaly detection, additional research is necessary in this area.

5. Conclusions

Publicly available sensitive data should have adversarial threats prevented, and privacy concerns in AI systems have to be dealt with using cryptographic techniques. The

recent interest in this topic has been reflected by the emphasis of a bibliometric analysis through the increase in publication evidence—especially in recent years. This research has demonstrated that AI security is an interdisciplinary area where cryptography is being combined with AI to handle emergent challenges in areas such as finance, health, and defense. The rapid growth in the number of publications from 2020 to 2024 underlines the need for securing AI models and systems when these are widely used in most industries.

The geographical distribution of research output in cryptographic techniques related to AI security is indicative of heavy contributors emanating from Asian nations, especially China and India. Other countries where reasonable contributions can be noted include Saudi Arabia, the United States, and the United Kingdom; these are leading not because of one reason but by investing hugely in AI and cybersecurity. This collaboration is hence very global in nature and of utmost importance, considering the problems most nations face in terms of integrity with regard to AI-driven processes and privacy. There is also increased interest and research effort in this area in the region, as represented by the emergence of countries such as South Korea, Taiwan, and Egypt as substantial players.

The major cryptographic techniques that are used in the research area to improve AI security are also revealed in the study. The most common among these are secure multi-party computation and homomorphic encryption, which have wide usages for offering solutions in performing computations while ensuring privacy preservation. Homomorphic encryption does encryption and processing of the data without decryption, so sensitive information will not be compromised during analysis. On the other hand, secure multiparty computation is considered a very promising approach to collaborative AI-driven systems since it allows several participants to jointly compute a function without revealing their private inputs. These methods are needed now, considering the ever-growing amount of sensitive personal data handled by AI applications as, in this respect, the demand for strong encryption methods is growing.

Large contributions by renowned authors and institutions underpin the importance of cross-disciplinary collaboration in order to be able to tackle such a complex security challenge that AI has brought forward. It is easy to see that future progress, as cryptography and AI continue to advance, will depend critically on these interdisciplinary efforts toward secure, privacy-preserving AI systems. Besides presenting urgently needed solutions to current issues, this ongoing research founds a basis for making future improvements possible in the sphere of AI security and, ultimately, enabling much more trustworthy and resilient AI-powered applications. The increasing intersection of cryptography and AI security underscores the need for robust, scalable encryption frameworks. The study identifies emerging trends, notably the rise in LLM security concerns post-2023, and calls for enhanced research in homomorphic encryption, federated learning, and post-quantum security. Future studies should emphasize practical implementations of cryptographic methods in real-time AI security frameworks.

Author Contributions: Conceptualization, H.T.; methodology, H.T.; validation, H.T., T.-V.L. and K.S.; formal analysis, H.T., T.-V.L. and K.S.; resources, H.T., T.-V.L. and K.S.; writing—original draft preparation, H.T.; writing—review and editing, T.-V.L. and K.S.; visualization, H.T.; supervision, H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Workman, M. Validation of a biases model in strategic security decision making. *Inf. Manag. Comput. Secur.* **2012**, *20*, 52–70. [CrossRef]

2. Li, F. The research on information safety problem of digital campus network. In Proceedings of the 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), Dengfeng, China, 8–10 August 2011; pp. 828–831.
3. Al Kuwaiti, A.; Nazer, K.; Al-Reedy, A.; Al-Shehri, S.; Al-Muhanna, A.; Subbarayalu, A.V.; Al Muhanna, D.; Al-Muhanna, F.A. A review of the role of artificial intelligence in healthcare. *J. Pers. Med.* **2023**, *13*, 951. [CrossRef] [PubMed]
4. Parmar, M. Xaisec-Explainable AI Security: An Early Discussion Paper on New Multidisciplinary Subfield in Pursuit of Building Trust in Security of AI Systems. 2021. Available online: https://osf.io/preprints/osf/rc92f_v1 (accessed on 3 March 2025).
5. Cintas-Canto, A.; Kaur, J.; Mozaffari-Kermani, M.; Azarderakhsh, R. ChatGPT vs. Lightweight security: First work implementing the NIST cryptographic standard ASCON. *arXiv* **2023**, arXiv:2306.08178.
6. Ganji, K.; Afshan, N. A bibliometric review of Internet of Things (IoT) on cybersecurity issues. *J. Sci. Technol. Policy Manag.* **2024**. Available online: https://www.emerald.com/insight/content/doi/10.1108/jstpm-05-2023-0071/full/html (accessed on 3 March 2025). [CrossRef]
7. Kumar, S.; Lim, W.M.; Sivarajah, U.; Kaur, J. Artificial intelligence and blockchain integration in business: Trends from a bibliometric-content analysis. *Inf. Syst. Front.* **2023**, *25*, 871–896. [CrossRef]
8. Perifanis, N.-A.; Kitsios, F. Investigating the influence of artificial intelligence on business value in the digital era of strategy: A literature review. *Information* **2023**, *14*, 85. [CrossRef]
9. Nasar, W.; Da Silva Torres, R.; Gundersen, O.E.; Karlsen, A.T. The use of decision support in search and rescue: A systematic literature review. *ISPRS Int. J. Geo-Inf.* **2023**, *12*, 182. [CrossRef]
10. Liu, X.; Wang, X.; Chang, J.; Zhang, H.; Cao, P. Landscape analysis and overview of the literature on oxidative stress and pulmonary diseases. *Front. Pharmacol.* **2023**, *14*, 1190817. [CrossRef]
11. Gauffriau, M. Counting methods introduced into the bibliometric research literature 1970–2018: A review. *Quant. Sci. Stud.* **2021**, *2*, 932–975. [CrossRef]
12. Jiang, W.; Sousa, P.S.; Moreira, M.R.; Amaro, G.M. Lean direction in literature: A bibliometric approach. *Prod. Manuf. Res.* **2021**, *9*, 241–263. [CrossRef]
13. Donthu, N.; Kumar, S.; Mukherjee, D.; Pandey, N.; Lim, W.M. How to conduct a bibliometric analysis: An overview and guidelines. *J. Bus. Res.* **2021**, *133*, 285–296. [CrossRef]
14. Bunjak, A.; Černe, M.; Schölly, E.L. Exploring the past, present, and future of the mindfulness field: A multitechnique bibliometric review. *Front. Psychol.* **2022**, *13*, 792599. [CrossRef] [PubMed]
15. Fang, X.; Ren, H.; Gu, M. Orbital angular momentum holography for high-security encryption. *Nat. Photonics* **2020**, *14*, 102–108. [CrossRef]
16. Taylor, P.J.; Dargahi, T.; Dehghantanha, A.; Parizi, R.M.; Choo, K.K.R. A systematic literature review of blockchain cyber security. *Digit. Commun. Netw.* **2020**, *6*, 147–156. [CrossRef]
17. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2489–2520. [CrossRef]
18. Khan, L.U.; Yaqoob, I.; Imran, M.; Han, Z.; Hong, C.S. 6G Wireless Systems: A Vision, Architectural Elements, and Future Directions. *IEEE Access* **2020**, *8*, 147029–147044. [CrossRef]
19. Sharma, A.; Vanjani, P.; Paliwal, N.; Basnayaka, C.M.W.; Jayakody, D.N.K.; Wang, H.C.; Muthuchidambaranathan, P. Communication and networking technologies for UAVs: A survey. *J. Netw. Comput. Appl.* **2020**, *168*, 102739. [CrossRef]
20. Anuradha, M.; Jayasankar, T.; Prakash, N.B.; Sikkandar, M.Y.; Hemalakshmi, G.R.; Bharatiraja, C.; Britto, A.S.F. IoT enabled cancer prediction system to enhance the authentication and security using cloud computing. *Microprocess. Microsyst.* **2021**, *80*, 103301. [CrossRef]
21. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 94668–94690. [CrossRef]
22. Li, B.; Feng, Y.; Xiong, Z.; Yang, W.; Liu, G. Research on AI security enhanced encryption algorithm of autonomous IoT systems. *Inf. Sci.* **2021**, *575*, 379–398. [CrossRef]
23. Sharma, P.; Jain, S.; Gupta, S.; Chamola, V. Role of machine learning and deep learning in securing 5G-driven industrial IoT applications. *Ad Hoc Netw.* **2021**, *123*, 102685. [CrossRef]
24. Jan, M.A.; Khan, F.; Khan, R.; Mastorakis, S.; Menon, V.G.; Alazab, M.; Watters, P. Lightweight Mutual Authentication and Privacy-Preservation Scheme for Intelligent Wearable Devices in Industrial-CPS. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5829–5839. [CrossRef]
25. Razdan, S.; Sharma, S. Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Tech. Rev. (Inst. Electron. Telecommun. Eng. India)* **2022**, *39*, 775–788. [CrossRef]

26. Hasan, M.K.; Ghazal, T.M.; Saeed, R.A.; Pandey, B.; Gohel, H.; Eshmawi, A.A.; Abdel-Khalek, S.; Alkhassawneh, H.M. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. *IET Commun.* **2022**, *16*, 421–432. [CrossRef]
27. Almaiah, M.A.; Hajjej, F.; Ali, A.; Pasha, M.F.; Almomani, O. An AI-Enabled Hybrid Lightweight Authentication Model for Digital Healthcare Using Industrial Internet of Things Cyber-Physical Systems. *Sensors* **2022**, *22*, 1448. [CrossRef]
28. Abdel Hakeem, S.A.; Hussein, H.H.; Kim, H. Security Requirements and Challenges of 6G Technologies and Applications. *Sensors* **2022**, *22*, 1969. [CrossRef] [PubMed]
29. Neelakandan, S.; Rene Beulah, J.; Prathiba, L.; Murthy, G.L.N.; Fantin Irudaya Raj, E.; Arulkumar, N. Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model. *Int. J. Model. Simul. Sci. Comput.* **2022**, *13*, 2241006. [CrossRef]
30. Rajapaksha, S.; Kalutarage, H.; Al-Kadri, M.O.; Petrovski, A.; Madzudzo, G.; Cheah, M. AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey. *ACM Comput. Surv.* **2023**, *55*, 1–40. [CrossRef]
31. Boualouache, A.; Engel, T. A Survey on Machine Learning-Based Misbehavior Detection Systems for 5G and Beyond Vehicular Networks. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1128–1172. [CrossRef]
32. Friha, O.; Ferrag, M.A.; Benbouzid, M.; Berghout, T.; Kantarci, B.; Choo, K.K.R. 2DF-IDS: Decentralized and differentially private federated learning-based intrusion detection system for industrial IoT. *Comput. Secur.* **2023**, *127*, 103097. [CrossRef]
33. Deebak, B.D.; Memon, F.H.; Khowaja, S.A.; Dev, K.; Wang, W.; Qureshi, N.M.F.; Su, C. A Lightweight Blockchain-Based Remote Mutual Authentication for AI-Empowered IoT Sustainable Computing Systems. *IEEE Internet Things J.* **2023**, *10*, 6652–6660. [CrossRef]
34. Ein Shoka, A.A.; Dessouky, M.M.; El-Sayed, A.; El-Din Hemdan, E. An efficient CNN based epileptic seizures detection framework using encrypted EEG signals for secure telemedicine applications. *Alex. Eng. J.* **2023**, *65*, 399–412. [CrossRef]
35. Almalawi, A.; Khan, A.I.; Alsolami, F.; Abushark, Y.B.; Alfakeeh, A.S. Managing Security of Healthcare Data for a Modern Healthcare System. *Sensors* **2023**, *23*, 3612. [CrossRef] [PubMed]
36. Dhar Dwivedi, A.; Singh, R.; Kaushik, K.; Rao Mukkamala, R.; Alnumay, W.S. Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Trans. Emerg. Telecommun. Technol.* **2024**, *35*, e4329. [CrossRef]
37. Gill, S.S. Quantum and blockchain based Serverless edge computing: A vision, model, new trends and future directions. *Internet Technol. Lett.* **2024**, *7*, e275. [CrossRef]
38. Alqaralleh, B.A.Y.; Vaiyapuri, T.; Parvathy, V.S.; Gupta, D.; Khanna, A.; Shankar, K. Blockchain-assisted secure image transmission and diagnosis model on Internet of Medical Things Environment. *Pers. Ubiquitous Comput.* **2024**, *28*, 17–27. [CrossRef]
39. Pleshakova, E.; Osipov, A.; Gataullin, S.; Gataullin, T.; Vasilakos, A. Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. *J. Comput. Virol. Hacking Tech.* **2024**, *20*, 429–440. [CrossRef]
40. Fang, W.; Zhu, C.; Zhang, W. Toward Secure and Lightweight Data Transmission for Cloud-Edge-Terminal Collaboration in Artificial Intelligence of Things. *IEEE Internet Things J.* **2024**, *11*, 105–113. [CrossRef]
41. Ishtaiwi, A.; Al Khaldy, M.A.; Al-Qerem, A.; Aldweesh, A.; Almomani, A. Artificial Intelligence in Cryptographic Evolution: Bridging the Future of Security. In *Innovations in Modern Cryptography*; IGI Global: Hershey, PA, USA, 2024; pp. 31–54.
42. Radanliev, P. Artificial intelligence and quantum cryptography. *J. Anal. Sci. Technol.* **2024**, *15*, 4. [CrossRef]
43. Sagar, R.; Jhaveri, R.; Borrego, C. Applications in security and evasions in machine learning: A survey. *Electronics* **2020**, *9*, 97. [CrossRef]
44. Pramanik, S.; Ghosh, R.; Ghonge, M.M.; Narayan, V.; Sinha, M.; Pandey, D.; Samanta, D. A novel approach using steganography and cryptography in business intelligence. In *Integration Challenges for Analytics, Business Intelligence, and Data Mining*; IGI Global Scientific Publishing: Hershey, PA, USA, 2021; pp. 192–217.
45. Dai, D.; Boroomand, S. A review of artificial intelligence to enhance the security of big data systems: State-of-art, methodologies, applications, and challenges. *Arch. Comput. Methods Eng.* **2022**, *29*, 1291–1309. [CrossRef]
46. Al-Suqri, M.N.; Gillani, M. A comparative analysis of information and artificial intelligence toward national security. *IEEE Access* **2022**, *10*, 64420–64434. [CrossRef]
47. Gulo, T.R.; Dwiastuti, I. The rising US trade protectionism under Donald Trump and its implication on China's artificial intelligence advancement. *AEGIS J. Int. Relat.* **2022**, *5*. [CrossRef]
48. Pise, A.A.; Almuzaini, K.K.; Ahanger, T.A.; Farouk, A.; Pant, K.; Pareek, P.K.; Nuagah, S.J. Enabling artificial intelligence of things (AIoT) healthcare architectures and listing security issues. *Comput. Intell. Neurosci.* **2022**, *2022*, 8421434. [CrossRef]
49. Hegde, S.B.; Srivastav, S.; Ks, N.B. A Comparative study on state of art Cryptographic key distribution with quantum networks. In Proceedings of the 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 7–9 October 2022; pp. 1–7.
50. Mao, B.; Kawamoto, Y.; Kato, N. AI-Based Joint Optimization of QoS and Security for 6G Energy Harvesting Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 7032–7042. [CrossRef]

51. Kim, A.; Park, M.; Lee, D.H. AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection. *IEEE Access* **2020**, *8*, 70245–70261. [CrossRef]
52. Yu, W.; Dillon, T.; Mostafa, F.; Rahayu, W.; Liu, Y. A global manufacturing big data ecosystem for fault detection in predictive maintenance. *IEEE Trans. Ind. Inform.* **2020**, *16*, 183–192. [CrossRef]
53. Yusuf, S.O.; Echere, A.Z.; Ocran, G.; Abubakar, J.E.; Paul-Adeleye, A.H.; Owusu, P. Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. *World J. Adv. Res. Rev.* **2024**, *23*, 2138–2147. [CrossRef]
54. Olasehinde, T. Real-Time Data Encryption and Decryption Using AI in Cloud Security. 2024. Available online: https://www.researchgate.net/publication/386178125_Real-Time_Data_Encryption_and_Decryption_Using_AI_in_Cloud_Security (accessed on 3 March 2025).
55. Ojo, B.; Aghaunor, C.T. AI-driven cybersecurity solutions for real-time threat detection in critical infrastructure. *Int. J. Sci. Res. Arch.* **2024**, *12*, 1716–1726.